[19]中华人民共和国国家知识产权局

[51]Int.Cl[7]
G06F 7/00

# [12]发明专利申请公开说明书

[21]申请号 99122085.4

[43]公开日 2000年8月16日

[11]公开号 CN 1263305A

[22]申请日 1999.10.28 [21]申请号 99122085.4
[30]优先权
[32]1999.2.9 [33]KR [31]4483/1999
[32]1999.2.9 [33]KR [31]4493/1999
[71]申请人 LG电子株式会社
地址 韩国汉城市
[72]发明人 曹英顺 金宰永 姜明俊 郑 翰

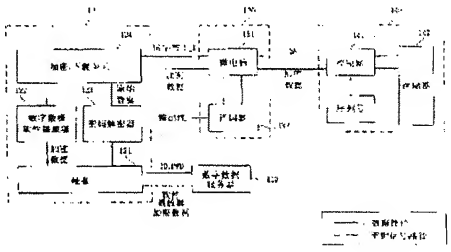
[74]专利代理机构 中原信达知识产权代理有限责任公司
代理人 余 朦

权利要求书2页 说明书8页 附图页数3页

[54]发明名称 数字数据文件加密装置和方法

[57]摘要

数字数据文件加密装置和方法。数字数据服务器识别用户身份并根据识别结果 将加密数字数据文件提供给该用户。个人电脑对由数字数据服务器所提供的加密数字数据文件进行解密,并重放解密所得的数字数据文件或利用密钥对其进 行再加密以将再加密数字数据文件下载。该密钥根据数据存储介质的ID号产 生。数字数据播放器将从个人电脑下载的再加密数字数据文件存储到数据存储 介质中,并利用该密钥对所存储的数字数据文件进行解密以进行重放。



ISSN1008-4274

# 权 利 要 求 书

1. 一种数字数据文件加密装置，包括：

数字数据服务器，用于识别用户身份并根据识别结果将加密数字数据文件提供给该用户；

个人电脑，其用于对由所述数字数据服务器提供的所述加密数字数据文件进行解密，并重放解密所得的数字数据文件，或利用密钥对其进行再加密以将再加密所得的数字数据文件下载，其中所述密钥是根据数据存储介质的 ID 号产生的；以及

数字数据播放器，用于将从所述个人电脑下载的所述再加密数字数据文件存储到所述数据存储介质中，并利用所述密钥对所存储的数字数据文件进行解密以对其进行重放。

2. 如权利要求 1 所述的装置，其特征在于所述密钥包括与制造公司名称，所述数据存储介质的序列号以及系统中所任意设置的数值有关的信息。

3. 一种用于对数字数据文件进行加密的方法，包括如下步骤：

a)输入数字数据播放器或与之相关的数据存储介质的 ID 号，并将第一预定内钥添加到所输入的 ID 号上以将所述 ID 号转换为一个密钥；

b)根据基于第二预定内钥的加密算法对所述密钥进行加密；

c)利用步骤 b)中加密所得的所述密钥对所述数字数据文件进行加密。

4. 如权利要求 3 所述的方法，其中所述第一预定内钥包括多个内钥。

5. 如权利要求 3 或 4 所述的方法，其中所述密钥包括与制造公司名称，所述数据存储介质的序列号以及系统中所任意设置的数值有

关的信息。

6. 如权利要求 3 所述的方法，其中所述加密算法与对所述数字数据文件进行加密所用的加密算法相同。

7. 如权利要求 3 所述的方法，其中由宿主机利用所述加密密钥对所述数字数据文件进行加密，而所述数字数据播放器则从所述宿主机接收加密数字数据文件并利用所述加密密钥对其进行解密，所述宿主机与数字数据播放器彼此共用所述第一和第二预定内钥以分别产生所述加密密钥。

8. 一种用于在其上记录数字数据文件加密程序的记录介质，该程序被设计成输入数字数据播放器或与之相关的数据存储装置的 ID 号，将第一预定内钥添加到所输入的 ID 号上以将所述 ID 号转换为一个密钥，根据基于第二预定内钥的加密算法对所述密钥进行加密，并利用所述加密密钥对数字数据文件进行加密。

# 说　明　书

## 数字数据文件加密装置和方法

本发明一般涉及防止通过诸如因特网等计算机通信网络进行传输的程序被非法下载和重放的技术，具体涉及对数字数据文件进行加密的装置和方法，即使数字数据文件在通过诸如因特网等类型的计算机通信网络传送到个人电脑和下载到数字数据播放器上的过程中被非法窃用（“hack”）了，也不会被恢复为其真实的数据流形式。

通常，MP3 是众多数字数据中的一种。而 MP3 播放器则是一种采用 MPEG1 Layer3 中所规定的音频数据压缩编码技术的新概念型、便携式数字设备，能够便捷地从计算机通信网络下载并重放所需数据。具体地说，由于其是以数字数据的形式来存储文件的，所以 MP3 播放器很少会出现故障且其音质极佳。另外，该种 MP3 播放器体积很小且重量很轻，从而其便携性很高，使得用户即使在进行体育锻炼时也可将其带在身上。因此，本产品作为便携磁带式录音机以及光盘（CD）随身听的替代产品正越来越受到业界的瞩目。

参照图 1，其所示为数字数据播放器及其相关外设的常规配置的方框图。图中，图注 10 表示数字数据服务器，在进行用户注册时其为个人电脑 20 指定标识（ID）号码和口令（PWD），并将软件形式的数字数据播放器 22 传送给个人电脑 20。一接收到来自用户的文件提供请求，数字数据服务器 10 便根据用户所输入的 ID 号和口令识别该用户的身份，并根据识别结果将加密数字数据文件提供给该用户。个人电脑 20 将由数字数据服务器 10 所提供的该数字数据文件存储于其硬盘 21 上，并通过所下载的软件播放器 22 对其进行解密以重放解密所得的未经处理的数字数据文件，或将其下载到数字数据播放器 30 上。数字数据播放器 30 从个人电脑 20 下载未经处理的数字数据文件，并将其存储在存储单元 40 中以对其进行重放。存储单元 40 从数字数

据播放器 30 下载未经处理的数字数据文件，并将其存储到其内部存储器 42 中，以在执行所需读取操作时进行输出。

接下来将对具有上述结构的常规配置的操作进行说明。

为了合法地从数字数据服务器 10 接收所需的数字数据文件，用户必须向数字数据文件提供者进行注册。为了进行用户注册，用户将由数字数据文件提供者指定一个 ID 号和口令。随后，用户通过通信网络从数字数据服务器 10 下载软件形式的数字数据播放器 22，并将所下载的数字数据软件播放器 22 安装到个人电脑 20 中。

随后，为了通过个人电脑 20 和通信网络从数字数据服务器 10 下载所需的数字数据文件，用户通过个人电脑 20 和通信网络将其 ID 号和口令传送给数字数据服务器 10。而数字数据服务器 10 则根据所传送来的 ID 号和口令识别用户的身份，并根据识别结果将所需的数字数据文件提供给该用户。其中数字数据服务器 10 以用户的 ID 号作为密钥对该数字数据文件进行加密，并将加密数字数据文件传送给个人电脑 20。

个人电脑 20 将从数字数据服务器 10 传送来的数字数据文件存储在硬盘 21 上。随后，一接收到来自用户的重放请求，个人电脑 20 便通过数字数据软件播放器 22 对所存储的数字数据文件进行解密及重放。其结果是，用户能够通过个人电脑 20 欣赏到所喜欢的音乐。

另一方面，如果用户想要利用便携式数字数据播放器 30 来欣赏数字数据文件形式的音乐，则个人电脑 20 将先利用数字数据软件播放器 22 对通过通信网络下载并存储于硬盘 21 上的该数字数据文件进行解密，再通过其下载单元 23 和通信网络将解密所得的数字数据文件传送给数字数据播放器 30。

随后，数字数据播放器 30 将沿上述路径传送来的数字数据文件存储到存储单元 40 的存储器 42（其被制成可拆卸存储器卡的形式）中。如果用户请求数字数据播放器 30 重放存储于存储器 42 中的数字数据文件，则数字数据播放器 30 将从存储器 42 中读出所存储的数字数据文件并通过其中的译码器 32 对其进行重放。其结果是，用户无论身在何处均能够通过数字数据播放器 30 欣赏其所喜欢的音乐。

然而，因为数字数据文件是在未经处理的情况下从个人电脑下载到数字数据播放器或进而再从数字数据播放器下载到存储器卡上的,所以如上所述的常规数字数据文件加密配置的缺点在于：数字数据文件可能会非法流出通信网络。数字数据文件诸如此类的非法流出将会使音乐版权所有者和音乐版权合作者（copyright associates）（比如负责音乐制作、复制和分销的音乐制作人和策划人）的版权权益得不到保护。

因此，本发明的初衷便在于解决上述问题，其一个目的是提供用于对数字数据文件进行加密的装置和方法，使得数字数据文件在从个人电脑下载到数字数据播放器上，进而从数字数据播放器下载到存储器卡中的过程中不会出现非法流出通信网络的现象。

本发明的另一个目的是提供一种数字数据文件加密装置和方法，其能够对密钥本身进行加密，使得即使从加密数字数据文件中非法提取出了密钥，也无法对该密钥进行解密，从而也就无法将数字数据文件恢复为其真实数据流。

根据本发明的一个方面，其提供了一种数字数据文件加密装置，其包括：数字数据服务器，用于识别用户身份并根据识别结果向用户提供加密数字数据文件；个人电脑，其用于对数字数据服务器所提供的加密数字数据文件进行解密，并重放解密所得的数字数据文件或利用一个密钥对其进行再加密，以将再加密所得的数字数据文件下载，

其中该密钥是根据数据存储介质的 ID 号产生的；和数字数据播放器，用于将从个人电脑下载来的再加密数字数据文件存储到数据存储介质中，并利用该密钥对所存储的数字数据文件进行解密以对其进行重放。

该密钥可优选包括与制造公司名称，数据存储介质的序列号和系统中所任意设置的数值有关的信息。

根据本发明的另一个方面，其提供了一种用于对数字数据文件进行加密的方法，其包括：第一步骤，输入数字数据播放器或与之相关的数据存储介质的 ID 号，以及将第一预定内钥添加到所输入的 ID 号上以将该 ID 号转换为一个密钥；第二步骤，根据基于第二预定内钥的加密算法对该密钥进行加密；以及第三步骤，利用在第二步骤加密所得的密钥对数字数据文件进行加密。

第一预定内钥可优选包括多个内钥，而密钥则可包括与制造公司名称，数据存储介质的序列号和系统中所任意设置的数值有关的信息。

另外，该加密算法可以和对数字数据文件进行加密所用的算法相同。

另外，由一台宿主机利用加密所得的密钥对数字数据文件进行加密，而数字数据播放器则从该宿主机接收加密数字数据文件，并利用加密密钥对其进行解密。为此，宿主机和数字数据播放器可以彼此共用第一和第二预定内钥以分别产生该加密密钥。

根据本发明的再一个方面，其提供了一种用于在其上记录数字数据文件加密程序的记录介质，该程序被设计成输入数字数据播放器或与之相关的数据存储介质的 ID 号，将第一预定内钥添加到所输入的 ID

号上以将该 ID 号转换为一个密钥，根据基于第二预定内钥的加密算法对该密钥进行加密，并利用加密所得的该密钥对数字数据文件进行加密。

从接下来结合附图所作的详细说明中将会对本发明的上述和其它目的、特性以及优点有更清楚地理解，其中：

图 1 所示为数字数据播放器及其相关多种外设的常规配置的方框图；

图 2 所示为根据本发明的用于数字数据播放器的数字数据文件加密装置的方框图；

图 3 所示为根据本发明的用于在数字数据播放器中对数字数据文件进行加密和解密的方法的方框图。

参照图 2，其所示为根据本发明的用于数字数据播放器的数字数据文件加密装置的结构方框图。接下来将对根据本发明的数字数据文件加密装置的操作进行详细说明。

首先，用户必须向一个数字数据文件提供者进行注册以从数字数据服务器 110 合法地接收所需的数字数据文件。为了进行用户注册，用户将由数字数据文件提供者指定一个 ID 号和口令（PWD）。随后，用户便通过通信网络从数字数据服务器 110 下载软件形式的数字数据播放器 122 并将所下载的数字数据软件播放器 122 安装到个人电脑 120 上。

随后，用户通过个人电脑 120 和通信网络将其 ID 号和口令传送给数字数据服务器 110 以通过个人电脑 120 和通信网络从数字数据服务器 110 下载所需的数字数据文件。数字数据服务器 110 根据所传送来的 ID 号和口令识别用户的身份，并根据识别结果将所需的数字数据文件提供给用户。与此同时，数字数据服务器 110 利用该用户的 ID 号作为密钥对数字数据文件进行加密，并将加密所得的数字数据文件

传送给个人电脑 120。个人电脑 120 则将从数字数据服务器 110 传送来的数字数据文件存储到其硬盘 121 上。随后，一旦接收到来自用户的重放请求，个人电脑 120 便通过数字数据软件播放器 122 对所存储的数字数据文件进行解密及重放。其结果是，用户能够通过个人电脑 120 欣赏其所喜欢的音乐。

另一方面，当用户想要利用数字数据播放器 130 来欣赏数字数据文件形式的音乐时，个人电脑 120 将通过数字数据播放器 130 和通信网络读出可拆卸式数据存储介质 140 的 ID 号，并根据所读出的 ID 号产生一个密钥。与此同时，数字数据播放器 130 也类似于个人电脑 120 利用数据存储介质 140 的 ID 号产生相同的密钥。

在个人电脑 120 中，密码解密器 123 对沿上述路径存储到硬盘 121 上的数字数据文件进行解密，而加密/下载单元 124 则利用该密钥对来自密码解密器 123 的解密数字数据文件进行再加密，并通过通信网络将再加密所得的数字数据文件传送给数字数据播放器 130。

数字数据播放器 130 将从个人电脑 120 下载的再加密数字数据文件存储到可拆卸式数据存储介质 140 的存储器 142 中。如果用户请求数字数据播放器 130 重放存储在存储器 142 中的数字数据文件，则数字数据播放器 130 将从存储器 142 中读出所存储的数字数据文件，并通过其译码器 132 对其进行重放。其中由于其为加密形式，所以将不得不先对从数据存储介质 140 中读出的数字数据文件进行解密以进行重放。

因此，在数字数据播放器 130 中，微电脑 131 利用根据数据存储介质 140 的 ID 号所产生的密钥对从数据存储介质 140 中读出的数字数据文件进行解密，并通过译码器 132 将解密所得的数字数据文件输出到输出线上。

其结果是，用户无论身在何处均能利用数字数据播放器 130 欣赏其所喜欢的音乐，而同时能够防止在数字数据文件被下载的过程中出现非法流出的现象。

很明显，可以有许多种利用数据存储介质 140 的 ID 号产生密钥的方法。例如，可以产生一个 16 字节长度的密钥 E_K，其中 3 个字节代表制造公司名称，12 个字节代表数据存储介质 140 的序列号 SN，1 个字节代表系统中所任意设置的数值。

图 3 所示为根据本发明的用于在数字数据播放器中对数字数据文件进行加密和解密的方法的方框图。首先，如果通过一个接口（未示出）将便携式 MP3 播放器 2 与个人电脑 1 连到一起，以从个人电脑 1 下载所需的数字数据文件，则个人电脑 1 将利用基于两装置之间协议的控制命令请求并输入与 MP3 播放器 2 或相关存储器（未示出）的 ID 号（序列号）有关的信息。

个人电脑 1 将所输入的 ID 号用作用户的认证号，因此使得不必再通过单独的用户认证处理。为了防止数据被窃取，个人电脑 1 将基于个人电脑 1 与便携式 MP3 播放器 2 两装置之间协议的第一内钥添加到所输入的 ID 号上，以将所输入的 ID 号转换为一个密钥。以此方式，可以对便携式 MP3 播放器 2 或相关存储器的 ID 号进行转换，以用作密钥。很明显，尽管文中只使用一个第一内钥，但也可以根据两装置之间的协议使用两个或更多的第一内钥，以使解密更加困难。

其应被注意的是转换所得的密钥通常被用来对数字数据文件进行加密。然而，在本发明中，将根据基于两装置之间协议的采用第二内钥的加密算法对转换所得的密钥自身进行加密，而随后再用其对数字数据文件进行加密。

尽管可以用密钥加密算法，而不是文件加密算法来对密钥进行加

密，但考虑到便携式 MP3 播放器 2 中所用的微处理器（未示出）的处理能力较低，所以优选采用文件加密算法，从而减小了用于存储算法的程序存储器的大小，且同时提高了处理的效率。

由于被进行下载的装置的 ID 号上添加了第一内钥，并且还以上述方式根据基于第二内钥的加密算法对所得密钥进行了加密，所以其将不能识别出密钥自身。随后则是以常规方式执行接下来的操作，以利用该加密密钥对数字数据文件进行加密，再将加密所得的数字数据文件传送给便携式 MP3 播放器 2。

以与个人电脑 1 相同的方式，便携式 MP3 播放器 2 通过将第一内钥添加到该装置的 ID 号上，并根据基于第二内钥的加密算法对所得密钥进行加密从而产生相同的加密密钥。随后，一接收到来自个人电脑 1 的加密数字数据文件，便携式 MP3 播放器 2 便根据基于该加密密钥的解密算法对所接收到的数字数据文件进行解密，并通过译码器输出解密所得的 MP3 文件。

正如从上述说明中所显而易见的，根据本发明，个人电脑和数字数据播放器均利用存储器卡的 ID 号产生相同的密钥，并根据所产生的密钥以能够防止下载过程中出现非法流出的方式对数字数据文件进行加密。具体地说，密钥自身也将被加密。因此，即使在传输过程中从文件流中非法提取出了该密钥，密钥也不能被解密，从而能够防止数字数据文件被窃取。

尽管上文中出于例示的目的公开了本发明的多种优选实施例，但对于本领域的技术人员来说，在不背离附加权利要求所公开的本发明的范围和精神的条件下可以对本发明进行多种形式地修正、添加和替换。

# 说 明 书 附 图

图1

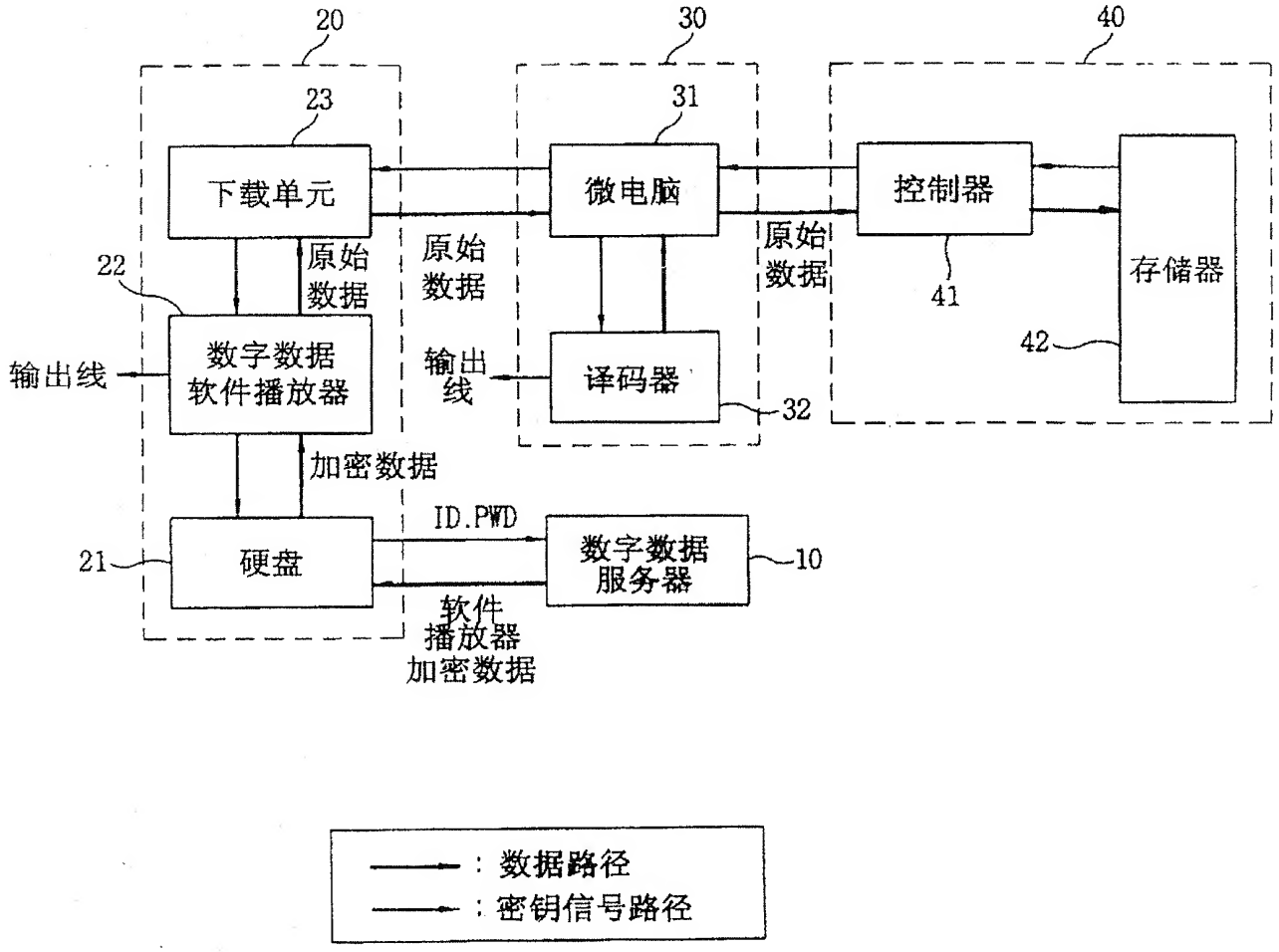
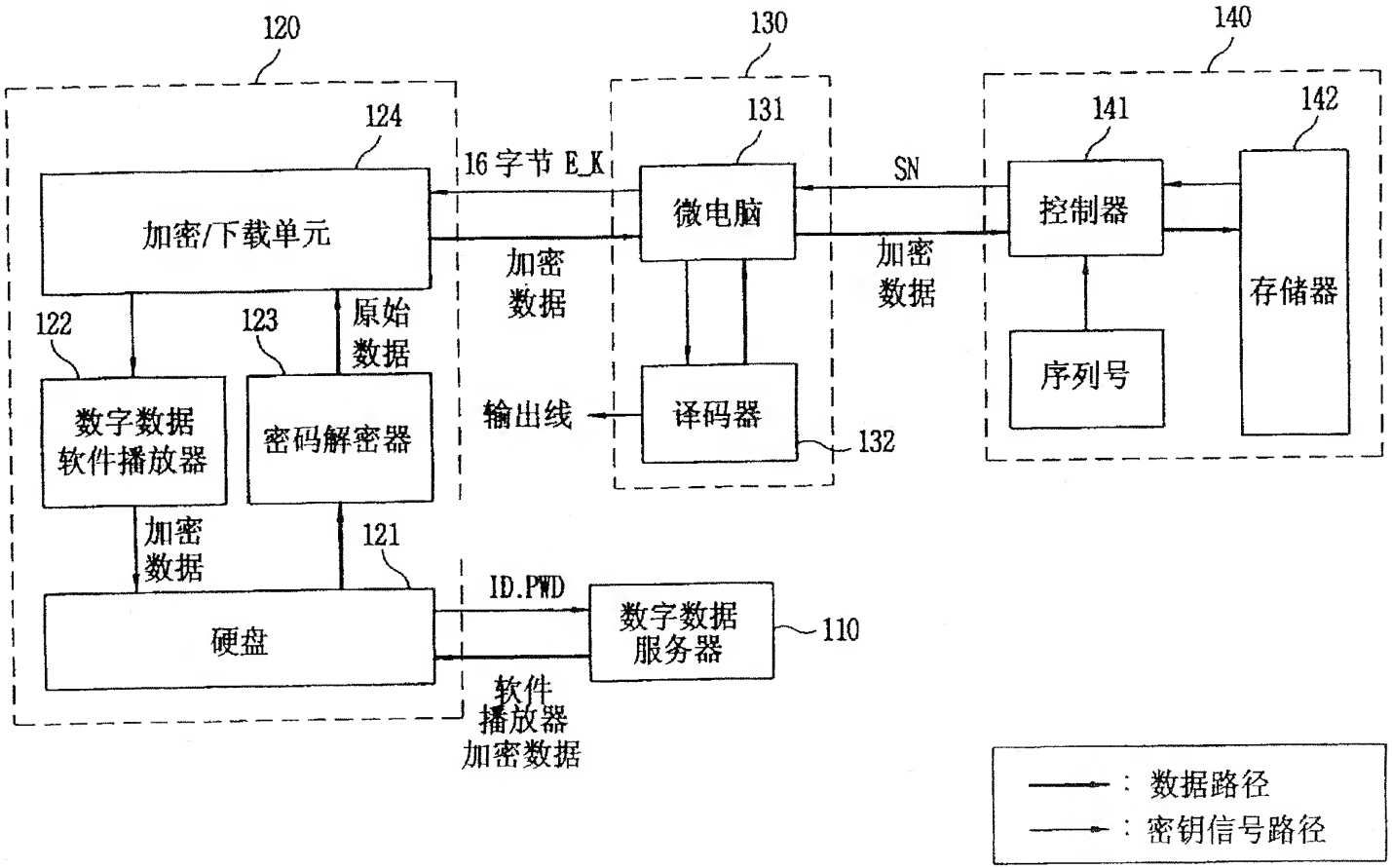
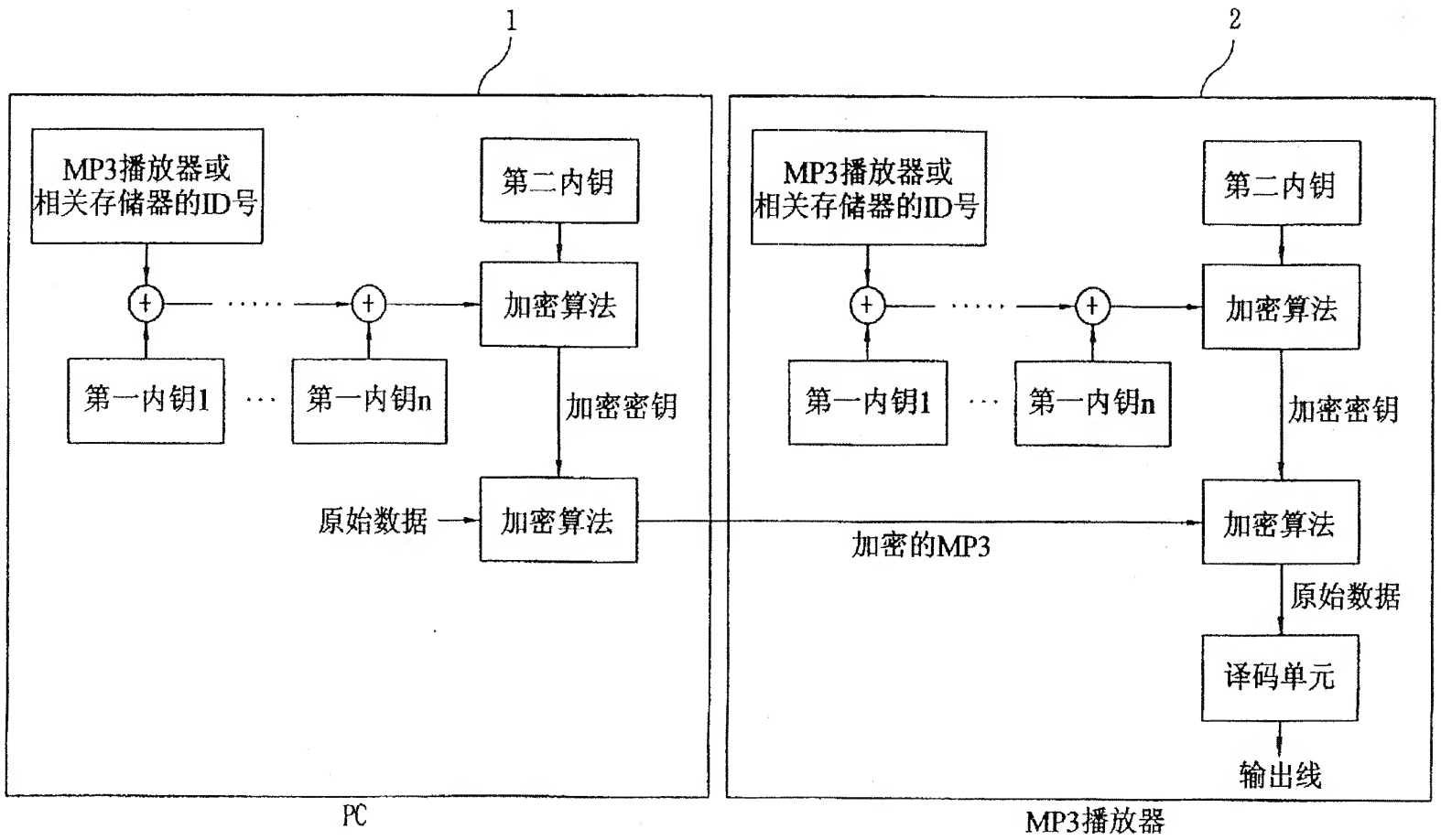

20
30
40
23
31
下载单元
微电脑
控制器
存储器
原始数据
原始数据
原始数据
22
41
42
数字数据软件播放器
输出线
输出线
译码器
32
加密数据
ID.PWD
21
硬盘
数字数据服务器
10
软件播放器加密数据
：数据路径
：密钥信号路径

图2


120
130
140
124
131
141
142
16 字节 E_K
SN
加密/下载单元
微电脑
控制器
加密
数据
加密
数据
存储器
122
123
原始
数据
序列号
数字数据
软件播放器
密码解密器
输出线
译码器
132
加密
数据
121
ID.PWD
硬盘
数字数据
服务器
110
软件
播放器
加密数据
：数据路径
：密钥信号路径

# 图3


1
2
MP3播放器或
相关存储器的ID号
第二内钥
加密算法
第一内钥1
第一内钥n
加密密钥
原始数据
加密算法
PC
MP3播放器或
相关存储器的ID号
第二内钥
加密算法
第一内钥1
第一内钥n
加密密钥
加密的MP3
加密算法
原始数据
译码单元
输出线
MP3播放器